

pu03-107

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-259223  
(P2002-259223A)

(43) 公開日 平成14年9月13日 (2002.9.13)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テーマコード(参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 F 5 B 0 1 7
15/00	3 3 0	15/00	3 3 0 Z 5 B 0 8 5
17/60	Z E C	17/60	Z E C 5 C 0 6 4
	1 4 2		1 4 2 5 J 1 0 4
	3 0 2		3 0 2 E

審査請求 有 請求項の数18 O L (全 12 頁) 最終頁に続く

(21) 出願番号 特願2001-53193(P2001-53193)

(22) 出願日 平成13年2月27日 (2001.2.27)

(71) 出願人 390009531

インターナショナル・ビジネス・マシーンズ・コーポレーション  
INTERNATIONAL BUSINESS MACHINES CORPORATION  
アメリカ合衆国10504、ニューヨーク州  
アーモンク ニュー オーチャード ロード

(74) 復代理人 100112520

弁理士 林 茂則 (外2名)

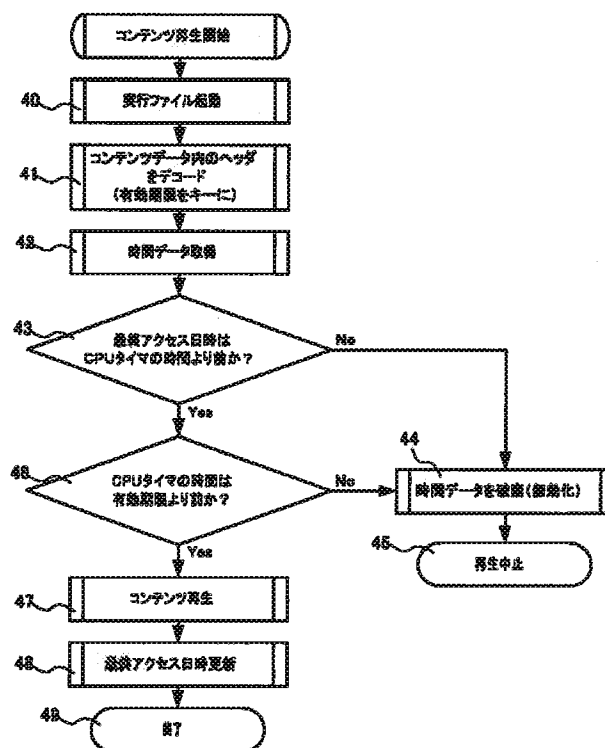
最終頁に続く

(54) 【発明の名称】 コンテンツ利用方法、コンテンツ配信方法、コンテンツ配信システムおよびプログラム

(57) 【要約】

【課題】 コンテンツ利用に有効期限を設けた場合に、ユーザの不正なコンテンツ利用を防止する。

【解決手段】 コンテンツまたはコンテンツ実行プログラムに有効期限を示す情報を持たせる。有効期限情報は、たとえば外部ファイル、コンテンツまたはコンテンツ実行プログラムに埋め込む。また、有効期限情報は、利用開始日時、利用終了日時、最終利用日時とする。これらデータを認証データとして、コンテンツの利用時(コンテンツ実行プログラムの実行時)に認証を行う。認証の手法として、たとえば、コンテンツ利用の際に、  
(1) システムタイマから取得される現在日時が利用開始日時と利用終了日時(有効期限)の間にあること、  
(2) 現在日時が最終利用日時(最終アクセス日時)よりあとであること、の2つの要件を満足する場合にのみ実行プログラムの実行を許可する。



## 【特許請求の範囲】

【請求項1】 コンテンツの利用開始日時を特定する利用開始日時と、コンテンツ利用の有効期限を特定する利用終了日時と、コンテンツが最後に利用された日時を特定する最終利用日時とを含む認証データを取得するステップと、

コンテンツの利用に際して、現在日時をシステムタイマから取得するステップと、

前記最終利用日時が前記現在日時より前であるかを判断する第1判断ステップと、

前記現在日時が、前記利用終了日時より前であるかを判断する第2判断ステップと、

前記第1および第2判断ステップの何れのステップにおいても、その判断が真の場合に前記コンテンツを再生または実行するステップと、

前記コンテンツの再生または実行の終了により、その終了日時で前記最終利用日時を更新するステップと、を有するコンテンツの利用方法。

【請求項2】 前記コンテンツの全体または一部が、前記認証データに含まれる暗号化データで符号化されており、

符号化されたコンテンツを前記暗号化データで復号化するステップをさらに有する請求項1記載のコンテンツの利用方法。

【請求項3】 前記第1判断ステップまたは第2判断ステップの何れかのステップにおいて、その判断が偽の場合、前記暗号化データを破棄するステップをさらに有する請求項2記載のコンテンツの利用方法。

【請求項4】 前記認証データは、隠しファイルとして生成されたファイル内に格納される第1の方法、または、前記コンテンツに埋め込まれる第2の方法、または、前記コンテンツを再生または実行するプログラムに埋め込まれる第3の方法、の何れかの方法で記録される請求項1記載のコンテンツの利用方法。

【請求項5】 コンテンツのダウンロード要求に応答して、前記要求を受け付けた時刻を用いてコンテンツの利用開始日時を特定する利用開始日時と、コンテンツ利用の有効期限を特定する利用終了日時とを含む認証データを生成するステップと、

前記コンテンツ、前記コンテンツの再生または実行プログラムおよび前記認証データ、または、これらを符号化したファイルを送信するステップと、を有し、

前記再生または実行プログラムは、その処理実行に際して、

現在日時をシステムタイマから取得する機能と、前記コンテンツの最終利用日時が前記現在日時より前であるかを判断する第1判断機能と、

前記現在日時が、前記利用終了日時より前であるかを判断する第2判断機能と、

前記第1および第2判断の何れの判断においてもその判

断が真の場合に前記コンテンツを再生または実行する機能と、

前記コンテンツの再生または実行の終了により、その終了日時で前記最終利用日時を更新する機能と、をコンピュータに実現させるものである、

コンテンツ配信方法。

【請求項6】 前記コンテンツの全部または一部を前記認証データに含まれる暗号化データで符号化するステップをさらに有し、

10 前記再生または実行プログラムは、前記符号化されたコンテンツを前記暗号化データを用いて復号化する機能をさらに有するものである請求項5記載のコンテンツ配信方法。

【請求項7】 前記再生または実行プログラムは、前記第1判断機能または第2判断機能において、その判断が偽の場合、前記暗号化データを破棄する機能をさらに有するものである請求項6記載のコンテンツ配信方法。

【請求項8】 前記認証データは、前記再生または実行プログラムが実行されるシステムの隠しファイルとして生成されたファイル内に格納される第1の方法、または、前記コンテンツに埋め込まれる第2の方法、または、前記再生または実行するプログラムに埋め込まれる第3の方法、の何れかの方法で記録される請求項5記載のコンテンツ配信方法。

【請求項9】 コンテンツのダウンロード要求に応答して、前記要求を受け付けた時刻を用いてコンテンツの利用開始日時を特定する利用開始日時と、コンテンツ利用の有効期限を特定する利用終了日時とを含む認証データを生成する手段と、

30 前記コンテンツ、前記コンテンツの再生または実行プログラムおよび前記認証データ、または、これらを符号化したファイルを送信する手段と、を有し、

前記再生または実行プログラムは、その処理実行に際して、

現在日時をシステムタイマから取得する機能と、前記コンテンツの最終利用日時が前記現在日時より前であるかを判断する第1判断機能と、

前記現在日時が、前記利用終了日時より前であるかを判断する第2判断機能と、

40 前記第1および第2判断の何れの判断においてもその判断が真の場合に前記コンテンツを再生または実行する機能と、

前記コンテンツの再生または実行の終了により、その終了日時で前記最終利用日時を更新する機能と、をコンピュータに実現させるものである、

コンテンツ配信システム。

【請求項10】 前記コンテンツの全部または一部を前記認証データに含まれる暗号化データで符号化する手段をさらに有し、

50 前記再生または実行プログラムは、前記符号化されたコ

ンテンツを前記暗号化データを用いて復号化する機能をさらに有するものである請求項9記載のコンテンツ配信システム。

【請求項11】 前記再生または実行プログラムは、前記第1判断機能または第2判断機能において、その判断が偽の場合、前記暗号化データを破棄する機能をさらに有するものである請求項10記載のコンテンツ配信システム。

【請求項12】 前記認証データは、前記再生または実行プログラムが実行されるシステムの隠しファイルとして生成されたファイル内に格納される第1の手段、または、前記コンテンツに埋め込まれる第2の手段、または、前記再生または実行するプログラムに埋め込まれる第3の手段、の何れかの手段で記録される請求項9記載のコンテンツ配信システム。

【請求項13】 コンテンツの利用開始日時を特定する利用開始日時と、コンテンツ利用の有効期限を特定する利用終了日時と、コンテンツが最後に利用された日時を特定する最終利用日時とを含む認証データを取得する機能と、

現在日時をシステムタイマから取得する機能と、前記最終利用日時が前記現在日時より前であるかを判断する第1判断機能と、前記現在日時が、前記利用終了日時より前であるかを判断する第2判断機能と、前記第1および第2判断機能の何れの判断においてもその判断が真の場合に前記コンテンツを再生または実行する機能と、前記コンテンツの再生または実行の終了により、その終了日時で前記最終利用日時を更新する機能と、をコンピュータに実現させるコンテンツを利用するためのプログラム。

【請求項14】 前記コンテンツの全体または一部が、前記認証データに含まれる暗号化データで符号化されており、前記プログラム製品が、符号化されたコンテンツを前記暗号化データで復号化する機能と、前記第1判断機能または第2判断機能の何れかの判断において、その判断が偽の場合、前記暗号化データを破棄する機能と、をさらに有する請求項13記載のプログラム。

【請求項15】 前記コンテンツを利用するコンピュータシステムに、そのシステムの稼働中または前記システム上で稼働するOSの稼働中に常時稼働しているカウンタ機能を実現するプログラムを有し、前記システムの稼働開始または前記OSの稼働開始の際に、前記プログラムで実現されたカウンタの時刻をシステムタイマから取得した日時で初期化するステップと、前記コンテンツの利用の際に、前記カウンタによる日時

とシステムタイマから取得した日時との差分を記録するステップと、

前記差分に相当する期間で、前記最終利用日時および前記利用終了日時、または、前記現在日時を補正するステップと、

をさらに含む請求項1記載のコンテンツ利用方法。

【請求項16】 前記コンテンツ、前記コンテンツの再生または実行プログラムおよび前記認証データ、または、これらを符号化したファイルを送信するステップにおいて、システムの稼働中または前記システム上で稼働するOSの稼働中に常時稼働しているカウンタ機能を実現するプログラムを同時に送付し、

前記カウンタ機能を実現するプログラムは、前記システムの稼働開始または前記OSの稼働開始の際に、前記カウンタ機能による時刻をシステムタイマから取得した日時で初期化する機能と、前記システムタイマとは独立に時刻をカウントする機能とをコンピュータに実現させるものであり、

前記再生または実行プログラムは、その処理に際して、前記カウンタ機能による日時とシステムタイマから取得した日時との差分を記録する機能と、前記差分に相当する期間で、前記最終利用日時および前記利用終了日時、または、前記現在日時を補正する機能と、をさらにコンピュータに実現させるものである請求項5記載のコンテンツ配信方法。

【請求項17】 前記コンテンツ、前記コンテンツの再生または実行プログラムおよび前記認証データ、または、これらを符号化したファイルを送信する手段において、システムの稼働中または前記システム上で稼働するOSの稼働中に常時稼働しているカウンタ機能を実現するプログラムを同時に送付し、

前記カウンタ機能を実現するプログラムは、前記システムの稼働開始または前記OSの稼働開始の際に、前記カウンタ機能による時刻をシステムタイマから取得した日時で初期化する機能と、前記システムタイマとは独立に時刻をカウントする機能とをコンピュータに実現させるものであり、

前記再生または実行プログラムは、その処理に際して、前記カウンタ機能による日時とシステムタイマから取得した日時との差分を記録する機能と、前記差分に相当する期間で、前記最終利用日時および前記利用終了日時、または、前記現在日時を補正する機能と、をさらにコンピュータに実現させるものである請求項9記載のコンテンツ配信システム。

【請求項18】 システムの稼働開始または前記OSの稼働開始の際に、前記カウンタ機能による時刻をシステムタイマから取得した日時で初期化する機能と、前記システムタイマとは独立に時刻をカウントする機能とをコンピュータに実現させるカウンタプログラムから日時を取得する機能と、

前記カウンタプログラムによる日時とシステムタイマから取得した日時との差分を記録する機能と、前記差分に相当する期間で、前記最終利用日時および前記利用終了日時、または、前記現在日時を補正する機能と、をさらにコンピュータに実現させる請求項13記載のプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンテンツの配信方法、システムおよびそれらを実現するソフトウェアに関し、特に、コンテンツの利用に有効期限を設ける場合に適用して有効な技術に関する。

【0002】

【従来の技術】インターネット等、ネットワーク技術の進展により、画像、映像、音声、アプリケーションソフトウェア等のデジタルコンテンツのネットワーク配信が商業ベースで行われるようになってきている。これらデジタルコンテンツのネットワーク配信は、CD-ROM等の媒体にコンテンツを記録して販売される場合のように、媒体の製造、在庫、流通、店頭による販売等が必要でなく、デジタルコンテンツ（情報）の販売を拡大する有望な手法として期待される。すなわちネットワーク配信では情報をやり取りするだけでユーザにコンテンツを渡すことができ、適当な決済手段を併用することにより、ほぼ自動的にコンテンツの直接販売を完了できる。販売側は人員、設備、資産等の経営資源を削減でき、一方ユーザにとっては任意の場所で好きな時間に迅速にコンテンツを入手することができる。コンテンツのネットワーク配信は、両者にとってその利便性が極めて高く、販売コストの削減、ひいては販売価格の低減を図ることが可能になる。

【0003】しかしながらデジタルコンテンツはデジタル情報であるため本質的に複製が可能であり、複製による品質の劣化が極めて少ない。また、複製されたコンテンツは、ネットワークを用いればほぼ瞬時に世界的な規模で流布することが可能であり、コンテンツ所有者の著作権等の利益を大きく侵害することになる。このため、複製防止の技術が重要であり、一般に各種の認証手段をコンテンツの実行プログラムに備えて、認証を得たもののだけが実行プログラムを起動してコンテンツを利用できるようにしている。

【0004】一方、コンテンツの利用には有効期限が設けられる場合がある。たとえば特定目的のアプリケーションソフトウェアを試用期間として配布する場合や、廉価に配布されるシェアウェアの場合である。あるいは、課金目的に音楽ソフトや映画等の映像ソフトを配信する場合にも有効期限が設けられる場合がある。このように有効期限を設けてコンテンツを販売することにより、コンテンツの利用の機会を拡大し、あるいはコンテンツ利

用の料金を安くして、コンテンツの利用促進を図ることが可能になる。

【0005】コンテンツに有効期限を設けるには、たとえばコンテンツあるいはコンテンツ実行プログラムに有効期限情報を持たせ、プログラムを実行するコンピュータ等情報処理装置のシステムタイマを用いて期限が経過しているか否かを判断する手法が一般的である。なお、インターネットからの配信データに有効期限を付す技術として、たとえば特開平11-31130号公報に記載の技術がある。

【0006】

【発明が解決しようとする課題】しかしながら、前記した従来技術のみでは、利用者の不正使用を簡単に許す場合がある。すなわち、前記複製防止手段によりコンテンツあるいはその実行プログラムの不正な複製は防止できる。ところが、複製防止手段だけではコンテンツの利用に有効期限を設けた場合の不正な使用を有効に防止できない。つまり、従来技術においては、コンテンツ利用の有効期限をその実行プログラムが走るコンピュータのシステムタイマを用いて判断するので、ユーザが故意にシステムタイマを変更してその日時を有効期限内に戻した場合には、実際には有効期限を渡過した場合であってもコンテンツの利用・再生が可能になる。これではコンテンツ利用に有効期限を設けた意義がなくなってしまう。

【0007】本発明の目的は、コンテンツ利用に有効期限を設けた場合に、ユーザの不正なコンテンツ利用を防止する技術を提供することにある。

【0008】

【課題を解決するための手段】本願の発明の概略を説明すれば、以下の通りである。すなわち、本発明は、コンテンツまたはコンテンツ実行プログラムに有効期限を示す情報を持たせる。有効期限情報は、たとえば外部ファイル、コンテンツまたはコンテンツ実行プログラムに埋め込むことができる。また、有効期限情報は、利用開始日時、利用終了日時（有効期限）、最終利用日時とすることができ、これらデータを認証データとして、コンテンツの利用時（コンテンツ実行プログラムの実行時）に認証を行うことができる。認証の手法として、たとえば、コンテンツ利用の際に、（1）システムタイマから取得される現在日時が利用開始日時と利用終了日時の間にあること（あるいは現在日時が利用終了日時前であること）、（2）現在日時が最終利用日時よりあとであること、の2つの要件を満足する場合にのみ実行プログラムの実行を許可することにより行う。

【0009】このようなコンテンツの実行方法を用いることにより、有効期限内でのコンテンツの利用が許可されるとともに、仮にユーザが不正にシステムタイマを戻しても、前記（2）の要件を満たさない場合には、コンテンツの利用を制限することができ、有効期限が付されたコンテンツの不正な利用を防止できる。

【0010】また、本発明では、システムタイマとは独立にそのシステムまたはOSの稼動中に独立した時刻をカウントするカウンタを設け、コンテンツ実行の際に、このカウンタから取得した時刻とシステムタイマの時刻とに差がある場合には、この差分に相当する期間で利用終了日時（有効期限）を補正することができる。これにより、最終利用日時と利用終了日時（有効期限）の間をターゲットにした時刻変更による不正使用の継続を防止できる。

#### 【0011】

【発明の実施の形態】以下、本発明の実施の形態を図面に基いて詳細に説明する。ただし、本発明は多くの異なる態様で実施することが可能であり、本実施の形態の記載内容に限定して解釈すべきではない。なお、実施の形態の全体を通して同じ要素には同じ番号を付するものとする。

【0012】以下の実施の形態では、主に方法またはシステムについて説明するが、当業者であれば明らかなとおり、本発明はコンピュータで使用可能なプログラムとしても実施できる。したがって、本発明は、ハードウェアとしての実施形態、ソフトウェアとしての実施形態またはソフトウェアとハードウェアとの組合せの実施形態をとることができる。プログラムは、ハードディスク、CD-ROM、光記憶装置または磁気記憶装置等の任意のコンピュータ可読媒体に記録できる。

【0013】また以下の実施の形態では、一般的なコンピュータシステムを用いることができる。実施の形態で用いることができるコンピュータシステムは、中央演算処理装置（CPU）、主記憶装置（メインメモリ：RAM）、不揮発性記憶装置（ROM）、コプロセッサ、画像アクセラレータ、キャッシュメモリ、入出力制御装置（I/O）等、一般的にコンピュータシステムに備えられるハードウェア資源を備える。また、ハードディスク装置等の外部記憶装置、インターネット等のネットワークに接続可能な通信手段を備えることができる。コンピュータシステムには、パーソナルコンピュータ、ワークステーション、メインフレームコンピュータ等各種のコンピュータが含まれる。

【0014】図1は、本発明の一実施の形態であるコンテンツ配信方法を実現するシステムの一例を示した概念図である。本実施の形態のコンテンツ配信システムは、インターネット1に、コンテンツの配信を要求する端末、たとえばコンピュータシステム2、携帯電話3、携帯情報端末（PDA：Personal Digital Assistants）4と、コンテンツを配信するサーバ5とが接続されている。コンテンツ配信先端末（コンピュータシステム2、携帯電話3、携帯情報端末4：以下単に端末という）は、サーバ5に対し、コンテンツ配信要求を発生し、それに応じてサーバ5はコンテンツおよび認証データを端末に配信する。コンテンツおよび認証データを受信した端

末は、後に詳しく説明するような手段を用いてコンテンツの再生あるいは実行を行い、ユーザの利用に供する。

【0015】インターネット1は、良く知られているように、IP（Internet Protocol）に従って通信が行われる世界的に開かれたネットワークの一形態である。ここではインターネットを例示するが、他のネットワーク形態を利用することも可能である。たとえば専用電話線により接続されたネットワークあるいはCATV等のケーブルネットワークでもよい。インターネットの概念には、一般に利用が制限されるイントラネットも含む。また、ここではインターネット等の通信手段を介してサーバ5と端末とが接続される例を説明するが、ネットワークを介して前記要求および配信が行われる必要も無い。たとえば郵便、電話等によるユーザからの要求に応じて、サーバ5を管理する事業者が、たとえばCD-ROM等の媒体を介してコンテンツおよび認証データを配送してもよい。ただし、ネットワークを利用しない場合には、後述のダウンロードプログラムを利用できないので、後述の圧縮ファイルと認証データ2を配布することになる。

【0016】コンピュータシステム2は、前記した一般的なコンピュータシステムであり、インターネット1に接続するための一般的な通信手段を有する。携帯電話3は、電話機能に加え、たとえばiモード等インターネット対応のデータ通信機能を備える。携帯情報端末4は、一部の機能が制限されるものの基本的にはコンピュータシステム同様の機能を備え、インターネットに接続するための通信機能を備える。コンピュータシステム2、携帯電話3、携帯情報端末4には、たとえばHTTP（Hypertext Transfer Protocol）リクエストを発生する適当なブラウザソフトがインストールされていることが好ましい。サーバ5は、前記した一般的なコンピュータシステムであり、適当な通信手段を備える。

【0017】図2は、端末側のシステム（クライアント）とサーバ5のシステムを示したブロック図である。クライアント側のシステムには、たとえばブラウザ6、コンテンツ7、認証ファイル8、実行プログラム9、通信手段10を有する。サーバ側のシステムには、たとえば時間情報生成手段11、認証ファイル生成手段12、ダウンロードプログラムファイル生成手段13、圧縮ファイル生成手段14、コンテンツ15、通信手段16を有する。なお、図2のクライアント側のシステムは、ダウンロードプログラムファイルが実行された後の状態を示す。

【0018】クライアント側システムのブラウザ6は、インターネット1に接続し、サーバ5にHTTPリクエストを発生するために用いる。一般的なブラウザが例示できる。

【0019】コンテンツ7は、サーバ5からダウンロードされ、利用可能な状態にあるコンテンツデータであ

10

20

30

40

50

る。コンテンツには、たとえば音声ファイル、映像ファイル、アプリケーションプログラム等ユーザの利用対象のソフトウェア資源を例示できる。

【0020】認証ファイル8は、後に詳しく説明するように、コンテンツのダウンロードに際に参照される認証1データ、コンテンツの解凍の際に参照される認証2データ、コンテンツの再生・実行の際に参照される認証3データを含む。これら認証データは隠しファイルとして保存することが好ましい。隠しファイルとすることにより、ユーザの改ざんを防止することができる。また、隠しファイルとすることに加えて、この認証ファイルのエディットデート（ファイル生成、変更日時）をOSのインストール日時書き換えることも有効である。これによりユーザが隠しファイルを探査することを困難にし、その改ざんの防止をより有効にすることができる。

【0021】実行プログラム9は、コンテンツ7を再生・実行するためのプログラムである。たとえばMP3再生プログラム、MPEG再生プログラムや、アプリケーションプログラムを起動するためのプログラムが例示できる。

【0022】通信手段10は、サーバ5の通信手段16と協働してインターネット1を介してデータを通信する。

【0023】サーバ5の時間情報生成手段11は、クライアントからダウンロード要求があったときに、その時点の日時と有効期間後の日時（有効期限）を生成し、主に前記認証3データに含まれる利用開始日時および利用終了日時に相当するデータを生成する。

【0024】認証ファイル生成手段12は、前記した時間情報生成手段11により生成された時間情報から認証3データを生成し、また、前記認証1データおよび認証2データを自動的に生成する。認証1データは、圧縮されたコンテンツファイル（認証2データを含む）の格納先を示し、ダウンロードプログラムによって利用される。認証2データは、圧縮ファイルの解凍に用いられる。認証3データは、解凍されたコンテンツの利用（再生・実行）の際に用いられる。

【0025】ダウンロードプログラムファイル生成手段13は、後に説明する圧縮ファイルをダウンロードするためのプログラムファイルを生成する。ダウンロードプログラムファイルには、前記した認証1データが埋め込まれる。

【0026】圧縮ファイル生成手段14は、符号化された実行プログラム、認証3データおよびコンテンツを生成する。圧縮ファイルには前記した認証2データが埋め込まれる。実行プログラムおよびコンテンツの符号化は、認証2データを用いて復号化できるようにスクランブルをかける。スクランブルには、たとえばデータヒドゥン形式、ビットシフト形式を用いることができる。圧縮ファイルはクライアント側で実行した場合に自己解凍

形式で解凍されることが好ましい。また、圧縮ファイルは前記認証1データで指定されるアドレスに格納される。

【0027】コンテンツ15は、ユーザによる利用対象のソフトウェア資源である。本実施の形態では、コンテンツ15自体がユーザにダウンロードされるわけではない。

【0028】図3は、本実施の形態のコンテンツ配信方法の一例を示したフローチャートである。まず、クライアント側からサーバ5にコンテンツの配信リクエストを行う（ステップ20）。リクエストはたとえばHTTPリクエストである。

【0029】このリクエストを受け付けたサーバ5は、時間情報を生成する（ステップ21）。時間情報は、時間情報生成手段11によってサーバ5のシステムタイムを用いて生成される。前記要求を受け付けた日時（利用開始日時）、および、利用開始日時に有効期間を加えた日時（利用終了日時すなわち有効期限）が生成される。

【0030】次にサーバ5は、認証ファイル生成手段12によって認証ファイルを生成する（ステップ22）。認証ファイルには、前記のとおり認証1～3のデータがある。認証1データはサーバ内の任意のアドレスが指定され、認証2データはランダムに生成される。認証3データのうち利用開始日時、利用終了日時は前記時間情報生成手段によって生成された時間が適用される。認証3データのうち、最終利用日時（最終アクセス日時）は、未だ利用されていないので任意の値にできるが、ここでは利用開始日時とする。

【0031】次にサーバ5は、前記認証1データを埋め込んだダウンロードプログラムファイルをダウンロードプログラムファイル生成手段13により生成し、これをクライアントに送信する（ステップ23）。

【0032】さらに、サーバ5は、クライアントからの圧縮ファイル要求に備えて、圧縮ファイル生成手段14により圧縮ファイルを生成する。生成された圧縮ファイルは認証1データで指定されたアドレスに格納する（ステップ24）。

【0033】一方、ダウンロードプログラムファイルを受信したクライアントは、ダウンロードプログラムを起動する（ステップ25）。プログラムの起動は、受信完了により自動起動されても良い。

【0034】次に、クライアントはダウンロードプログラムファイルに埋め込まれた認証1データを認証ファイル8に格納し（ステップ26）、ダウンロードプログラムの処理にしたがって、圧縮ファイルのダウンロード要求を行う（ステップ27）。このとき、ダウンロード要求は、認証1データで参照されるアドレスに格納されているファイルをダウンロードするように行い、よって、認証1データで参照されるアドレスにファイルが存在しない場合には圧縮ファイルのダウンロードは行われな

い。つまり、ダウンロードプログラムを仮にユーザがコピーして第三者に渡しても、第三者は認証1データが格納された隠しファイルを持たないため圧縮ファイルのダウンロードはできない。これにより不正コピーされたダウンロードプログラムファイルが無効化し、第三者による不正コピーを防止できる。

【0035】圧縮ファイルの送信要求を受け付けたサーバ5は、認証1データで参照されるアドレスのファイルを送信する(ステップ28)。このファイルは前記ステップ24で処理されたとおりであれば、目的の圧縮ファイルであるはずである。

【0036】圧縮ファイルを受信するクライアントでは、圧縮ファイルから認証2データを分離し、この認証2データを隠しファイルに格納する(ステップ29)。圧縮ファイルの受信が完了すれば(ステップ30)、これを受けてサーバ5では認証1データを無効化する。これにより再度のあるいは不正なダウンロードを防止できる。

【0037】クライアントでは、圧縮ファイルのダウンロードの完了を受けて、その解凍処理が行われる(ステップ32)。解凍は、たとえば自己解凍形式で自動的に行われるようにしても良い。なお、この解凍の際、認証2データを参照することによりデコードされるようにする。このように認証2データを参照しなければ解凍できないようにすることにより、圧縮ファイルの不正コピーを防止できる。

【0038】圧縮ファイルの解凍により、クライアント側のシステムには、コンテンツ、認証3データ、および実行プログラムが利用可能な状態で保持される(ステップ33)。なお、実行プログラムは、認証2データを参照しなければ起動できないようにすることができる。これにより、解凍後のコンテンツの不正利用を防止することができる。

【0039】図4は、クライアント側におけるコンテンツの再生処理を説明するためのフローチャートである。まず、クライアントの端末は実行ファイルを起動する(ステップ40)。この起動の際に前記認証2データを参照することができることは前記のとおりである。

【0040】次に、コンテンツ内のヘッダを、有効期限を用いてデコードする(ステップ41)。なお、このデコードに対応するエンコードは予めコンテンツデータに施されているとする。このように有効期限を用いてコンテンツデータをエンコードしておけば、コンテンツのみの不正なコピーを防止することができる。

【0041】次に認証3データとして隠しファイルに格納された時間データを取得する(ステップ42)。この取得した時間データを用いて、最終アクセス日時(最終利用日時)がシステムタイマ(CPUタイマ)の時間より前かを判断する(ステップ43)。この判断がNoの時には、最終アクセス時間よりCPUタイマの方が先に

あるという正常使用の場合には本来生じない矛盾を生じる。このような場合、CPUタイマが不正に戻されたと判断して、時間データ(認証3データ)を破棄し(ステップ44)、再生を中止する(ステップ35)。このように認証3データ(時間データ)を破棄することにより、コンテンツデータのデコードが以後不可能になり、コンテンツの利用ができなくなる。

【0042】一方、ステップ43の判断がYesの場合、さらにCPUタイマの時間が有効期限より前か(有効期限内か)を判断する(ステップ46)。この判断がNoのとき、前記ステップ43でも判断がNoの場合と同様に認証3データを破棄したうえで再生を中止する。有効期限を経過したコンテンツの利用を制限したものである。

【0043】ステップ36の判断がYesの時、コンテンツを再生する(ステップ37)。前記ステップ33および36の判断を共にパスした場合のみ、有効期限内の正当使用と判断する。

【0044】コンテンツの再生後、認証データ3の最終アクセス日時(最終利用日時)を更新する(ステップ38)。更新された最終利用日時は、次のコンテンツ利用の際に参照される。その後再生処理を終了する(ステップ39)。なお、コンテンツがダウンロードされた際に、最終利用日時としてダウンロード日時を記録することができる。

【0045】図5は、前記処理の流れを時系列に示した説明図である。ダウンロード時にダウンロード日時を最終利用日時としてデータファイル(認証3データ)に記録する。これを最終アクセス1とする。次に、時刻t1で再生を開始するときに図4の処理を行えば、再生開始時(現在時刻)は最終アクセス日時よりあとであり、かつ有効期限内であるので、正常に再生が可能である。時刻t2で再生が終了すれば、その時刻が最終アクセス2の最終利用日時として記録される。

【0046】次に、時刻t3で再生される場合、時刻t1の場合と同様に再生が可能である。なお、再生途中で有効期限を経過しても、再生は最後まで行われる。

【0047】有効期限経過後の時刻t5で再生しようとした場合、現在時刻が有効期限(利用終了日時)を経過しているので、再生は不可能である。このとき、ユーザが不正に使用しようとしてシステムタイマ(CPUタイマ)をt7まで戻したとする。この場合、前記ステップ46の判断はパスするが、前記ステップ43の判断をパスしない。すなわち、前回の再生において、最終利用日時としてt4が最終アクセス3に記録されており、時刻t7が時刻t4より前になるという本来生じない矛盾を生じているためである。本実施の形態では、このような不正な利用を検出してこれを防止することが可能になる。

【0048】なお、たとえば図5において、2度目の再



生操作(t3~t4)を行わず、本来再生不可能な3度目の再生操作(t5~t6)におけるタイマの不正操作(現在時刻を戻す操作)を時刻t2と有効期限の間への変更として行った場合には、再生が可能であると共に最終利用日時が不正に繰り上がる。このような不正操作が繰返されれば、実質的な有効期限の延長が可能になる恐れがある。このような場合、以下のような対策を施すことができる。

【0049】すなわち、実行プログラム9と協働して作動しているたとえばDLL(dynamic link library)のような独立プログラムにシステムタイマとは別個のカウント手段を設ける。このような独立プログラムはシステムが稼動している間あるいは特定のOSが稼動している間は停止することがないので、コンピュータ(あるいはOS)が稼動する限り有効期限を消費するように機能させることができる。つまり独立プログラムによるカウンタは常にシステム立ち上げ(あるいはOS稼動開始)のときにシステムタイマによる現在時刻のアップデートを行う。実行プログラム9の実行開始時にシステムタイマの不正な時刻戻しが行われたかを判断し(不正なタイマ操作が行われたなら独立プログラムの時刻の方がシステムタイマより進むはずである)システムタイマを参照して不正操作分の期間を記録する。実行プログラム9の実行に際して、前記した最終アクセス日時と有効期限(あるいはCPUタイマ(システムタイマ)の取得値)に前記期間の補正を加える。このような補正を加えた後の時刻データを用いて前記処理を実行できる。なお、最終アクセス日時と有効期限に補正を加える場合は前記期間を元の日時から減ずる補正、CPUタイマの取得値に補正を加える場合は取得値に前記期間を加える補正を行う。これにより、正当な有効期限の判断が行える。なお、最終アクセス日時と有効期限に補正を加えた場合には補正後の最終アクセス日時および有効期限を記録し、CPUタイマの取得値に補正を加えた場合は前記期間を記録し、以後の実行プログラムの処理の際に参照する。また、独立プログラムは実行プログラム9が最初に実行されるときにインストールされ、以後そのシステムが稼動する時には常時稼動するように機能させることは勿論である。

【0050】以上、本発明者によってなされた発明を発明の実施の形態に基づき具体的に説明したが、本発明は前記実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更することが可能である。

【0051】たとえば、前記実施の形態では、認証1、2の各データおよび認証3の時刻データ(利用開始日時)を用いて各ファイルあるいはプログラムのコピー防止の手段を説明した。しかし、コピー防止は前記方法に限られず、その他各種の手法を用いることができる。たとえば電子透かしの技術等である。

【0052】また、前記実施の形態では、認証データの

記録方法として、別ファイル(隠しファイル)を用いて格納する方法を説明したが、これに限られない。たとえばコンテンツ自体に有効期限を埋め込む方法、あるいは、実行プログラム自体に有効期限を埋め込む方法を適用してもよい。

【0053】また、前記実施の形態において、再生途中でのシステムタイマの戻し操作を禁止するようにしても良い。

【0054】また、前記実施の形態では、クライアント側のシステムとして、コンピュータシステム2、携帯電話3、PDA4を例示したが、これに限られない。たとえばインターネット1に接続可能なビデオ再生機等を例示できる。この場合、ビデオデータのヘッダ領域に時間情報その他の認証データを埋め込み、この認証データを利用して前記した各種の認証を行うことができる。

【0055】また、前記した実施の形態では、コンテンツの配信要求に応答してサーバ5がコンテンツと必要な認証データを同時に送付する例を説明したが、コンテンツと認証データの配信時期を異ならせても良い。たとえば、クライアントからの要求に応じて、まず認証データ(有効期限情報とコンテンツを再生・実行するのに必要なデータ)を送付し、クライアントがコンテンツの再生・実行を望む時にその都度コンテンツを配信するオンデマンド配信を行っても良い。この場合、オンデマンド配信されたコンテンツは先に入手した認証データを用いて前記実施の形態に記載したような再生・実行処理(認証処理)を行い、コンテンツの利用が可能になる。また、事前に入手する認証データについては、所定範囲のコンテンツについて包括的に認証が与えられても良い。つまり認証データとコンテンツとは一対一に対応する必要はなく、複数のコンテンツあるいは将来提供される予定のコンテンツに対して1つの認証が与えられても構わない。

【0056】

【発明の効果】本願で開示される発明のうち、代表的なものによって得られる効果は、以下の通りである。すなわち、コンテンツ利用に有効期限を設けた場合に、ユーザの不正なコンテンツ利用を防止することができる。

【図面の簡単な説明】

【図1】本発明の一実施の形態であるコンテンツ配信方法を実現するシステムの一例を示した概念図である。

【図2】端末側のシステム(クライアント)とサーバ5のシステムを示したブロック図である。

【図3】本発明の一実施の形態であるコンテンツ配信方法の一例を示したフローチャートである。

【図4】クライアント側におけるコンテンツの再生処理を説明するためのフローチャートである。

【図5】前記処理の流れを時系列に示した説明図である。

【符号の説明】

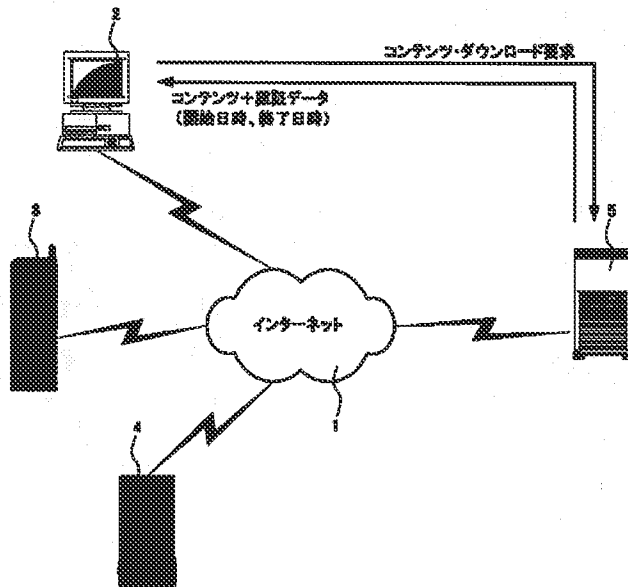
1…インターネット、2…コンピュータシステム、3…



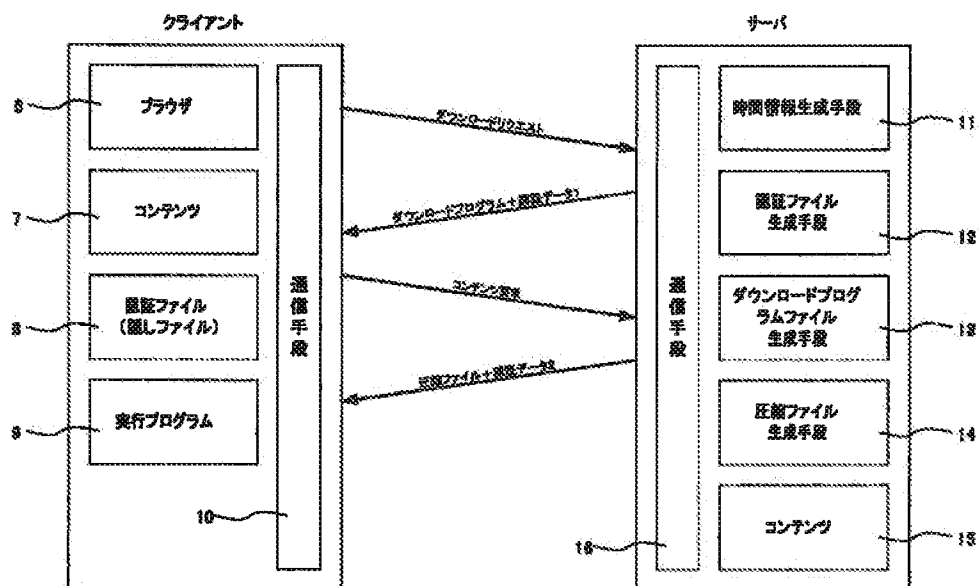
携帯電話、4…携帯情報端末、5…サーバ、6…ブラウザ、7…コンテンツ、8…認証ファイル、9…実行プログラム、10…通信手段、11…時間情報生成手段、12…認証ファイル生成手段、13…ダウンロードプログラム

\* ラムファイル生成手段、14…圧縮ファイル生成手段、15…コンテンツ、16…通信手段、t1～t7…時刻。

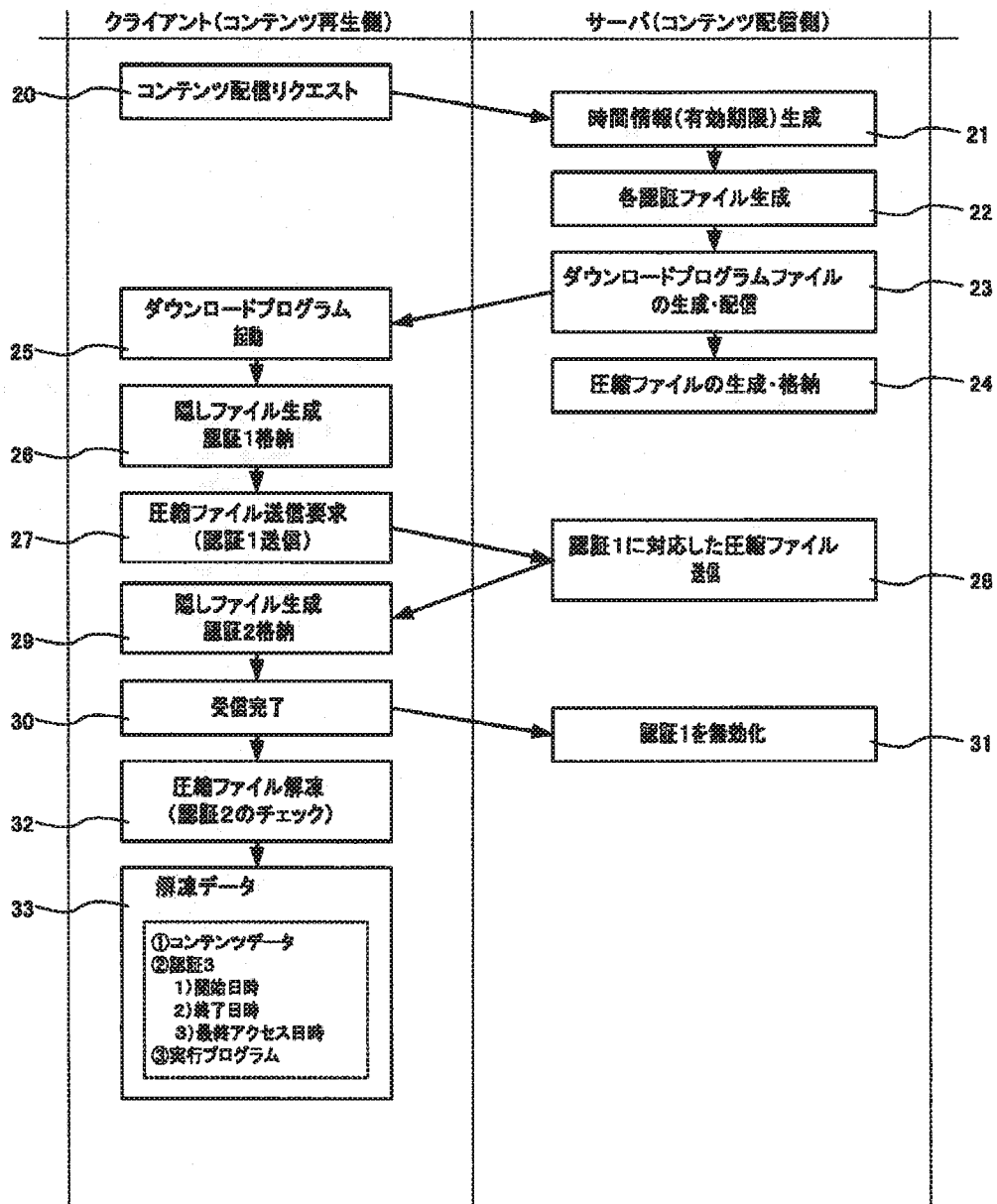
【図1】



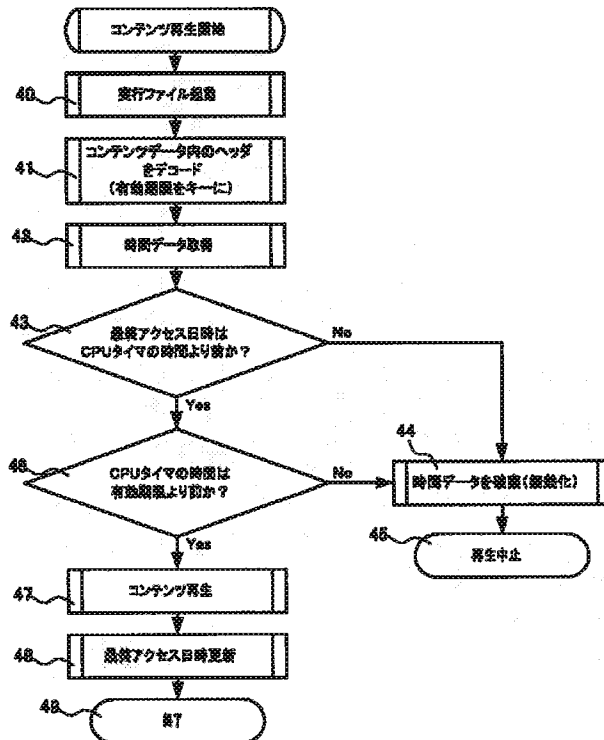
【図2】



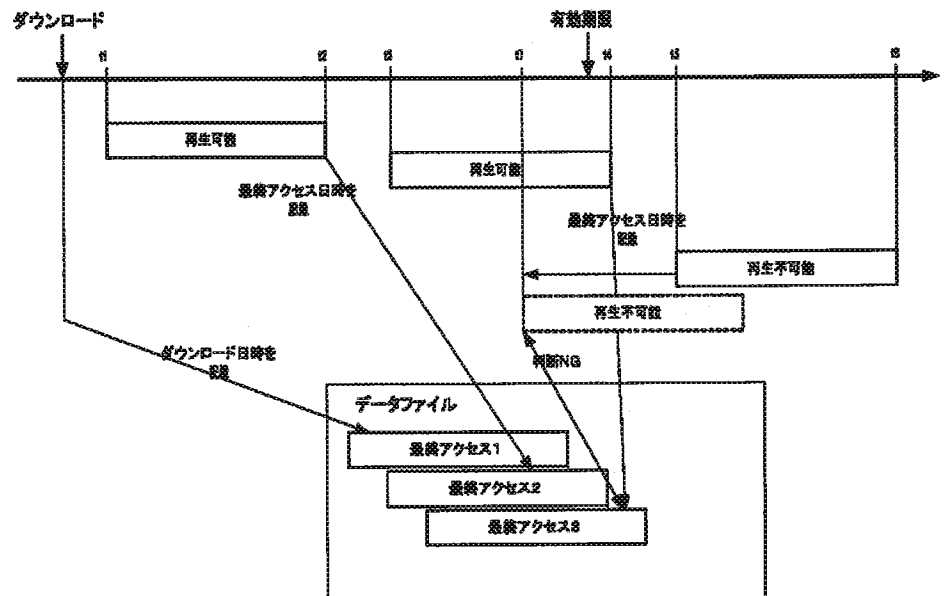
【図3】



【図4】



【図5】



フロントページの続き

(51)Int.Cl.

識別記号

FI

テーマコード(参考)

G 0 6 F 17/60

5 1 2

G 0 6 F 17/60

5 1 2

H 0 4 L 9/32

H 0 4 N 7/173

6 2 0 D

H 0 4 N 7/167

H 0 4 L 9/00

6 7 5 D

7/173

620

H04N 7/167

Z

(72)発明者 森 昌也

神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 大和事業所内

(72)発明者 岡本 順子

神奈川県大和市下鶴間1623番地14 日本ア  
イ・ビー・エム株式会社 大和事業所内

Fターム(参考) 5B017 AA07 BB10 CA15 CA16

5B085 AC05 AE23 BG07

5C064 BA07 BB10 BC17 BC18 BC22

BC23 BC25 BD02 BD08 BD09

CA14 CB01 CC04

5J104 AA07 AA14 KA02 PA14